ABSTRACT OF THE DISCLOSURE

The key management device manages keys respectively arranged on nodes forming an N-layer tree structure. Each group of keys composed of a key on the N^{th} layer and all its superordinate keys is assigned to a different reproducing device. Upon receipt of information designating a key group, the key selecting unit invalidates each key in the key group, and selects non-invalid keys immediately subordinate to each invalid key. The content encrypting unit encrypts a content using a content key. The ciphertext generating unit generates ciphertexts by encrypting the content key using each selected key. The selected key list generating unit generates a list of the selected keys used to encrypt the content key. The key management device records the encrypted data and the ciphertexts in a recording medium. The reproducing devices reads the recording medium, obtains the content key by decrypting s ciphertext using a key identified in the list.